ICS 35.240
CCS L67

团　　体　　标　　准

T/DGAG XXXX—XXXX

政务云平台建设技术要求

Technical requirements for construction of government cloud platform

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

广东省数字政务协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由广东省数字政务协会归口。

本文件起草单位：

本文件主要起草人：

政务云平台建设技术要求

1 范围

本文件给出了政务云平台整体技术要求，规定了政务云平台建设的机房环境要求、基础设施要求、支撑软件要求、业务应用要求、容灾备份要求、安全服务要求、运管平台与接口要求。

本文件适用于政务云管理部门、政务云使用单位、政务云服务商、政务云监管服务商及其他相关单位对政务云进行设计、建设、验收等活动。

区级政务云平台设计、建设等，也可参照本文件。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 50462 数据中心基础设施施工及验收规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 33780.1 基于云计算的电子政务公共平台技术规范 第1部分：系统架构

GB/T 33780.2 基于云计算的电子政务公共平台技术规范 第2部分：功能和性能

GB/T 33780.3 基于云计算的电子政务公共平台技术规范 第3部分：系统和数据接口

GB/T 33780.4 基于云计算的电子政务公共平台技术规范 第4部分：操作系统

GB/T 34077.3 基于云计算的电子政务公共平台管理规范 第3部分：运行保障管理

GB/T 34078.3 基于云计算的电子政务公共平台总体规范 第3部分：服务管理

GB/T 34078.4 基于云计算的电子政务公共平台总体规范 第4部分：服务实施

GB/T 34080.1 基于云计算的电子政务公共平台安全规范 第1部分：总体要求

GB/T 34080.2 基于云计算的电子政务公共平台安全规范 第2部分：信息资源安全

GB/T 34080.3 基于云计算的电子政务公共平台安全规范 第3部分：服务安全

GB/T 34080.4 基于云计算的电子政务公共平台安全规范 第4部分：应用安全

GB/T 36326 信息技术 云计算 云服务运营通用要求

3 术语和定义

GB/T 34078.1—2017界定的以及下列术语和定义适用于本文件。

3.1

政务云平台 government cloud

运用云计算技术，为行政事业单位提供基础设施、支撑软件、应用系统、信息资源、运行保障和信息安全等服务的资源平台。

3.2

政务云管理部门 government cloud management unit

依据职责负责政务云的规划建设和运行管理的单位。

3.3

政务云使用单位 government cloud user

政务云服务的使用方。

3.4

政务云服务商 government cloud service provider

政务云服务的供应方。

3.5

政务云监管服务商 government cloud supervision service provider

受政务云管理单位委托，开展政务云运维监管、安全监管、应急管理和服务评价等工作的参与方。

3.6

云管理平台 cloud management platform

管理云计算服务的控制台，是云计算服务监控、管理、分析和优化的重要工具，是支撑和保障的信息化架构。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

DDoS：分布式拒绝服务（Distributed Denial of Service）

HTTP：超文本传输协议（HyperText Transfer Protocol）

HTTPS：超文本传输安全协议（HyperText Transfer Protocol Secure）

IOPS：每秒的读写次数（Input/Output Operations Per Second）

IPv6：互联网协议第6版（Internet Protocol version 6）

MAC地址：媒体存取控制地址（Media Access Control Address）

TCP：传输控制协议（Transmission Control Protocol）

VPC：虚拟专有云（Virtual Private Cloud）

VPN：虚拟专用网络（Virtual Private Network）

5 总体框架

政务云平台总体框架图如图1，由机房环境、基础设施层、支撑软件层、业务应用层、云管平台与接口组成，并在安全和灾备体系的保障下，为政务云使用单位提供统一服务支撑。

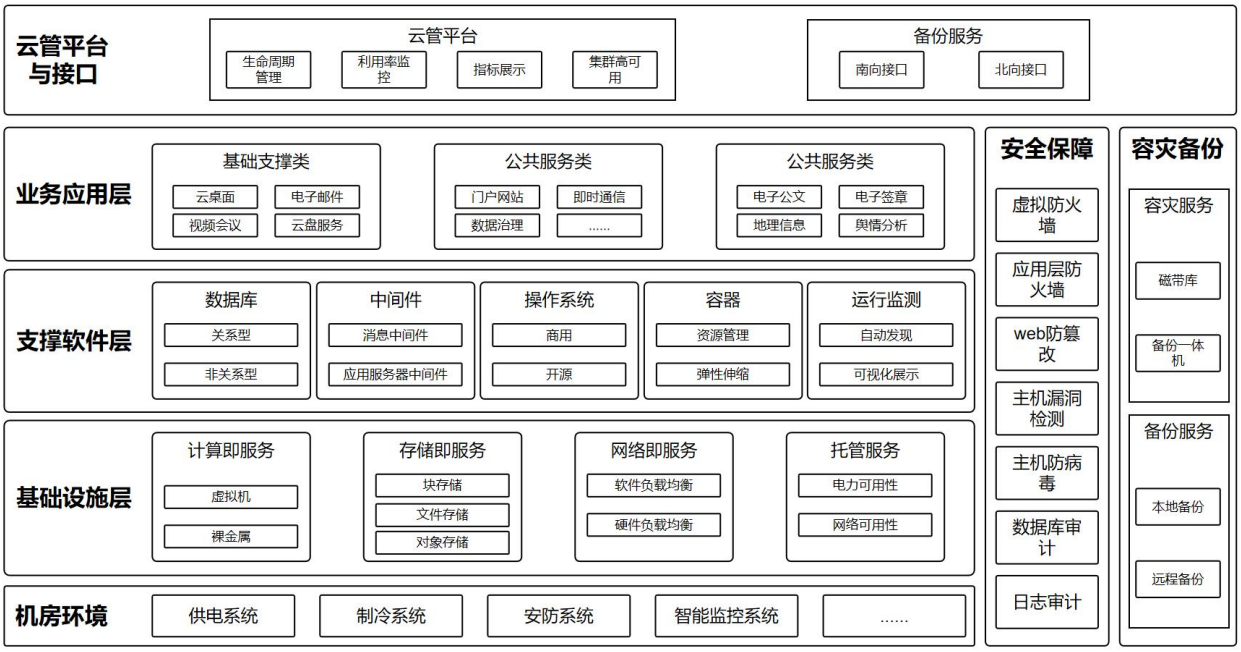

图 1　政务云平台技术框架图

应按如下内容设计具体架构：

a）　机房环境：为政务云提供安全、合规、完整的基础环境，应包含供电系统、制冷系统、安防系统、智能监控系统等；

b) 基础设施层：应遵循分层、分模块解耦、统一接口调用的建设原则，通过虚拟化技术将计算、存储和网络等硬件设备进行资源整合，为政务业务应用提供基础资源服务；
c) 支撑软件层：为各类政务业务应用的开发、测试、部署、运行和运维提供统一的支撑环境，保障业务稳定运行和敏捷迭代，包括但不限于容器、数据库服务、中间件服务以及操作系统服务等，并应支持统一管理；
d) 业务应用层：为满足政务云使用单位业务需求，政务云平台可提供共性的业务应用服务，如云盘、数据治理工具等；
e) 容灾备份服务。为政务云提供本地数据备份和恢复的能力，支持数据级容灾服务，保障业务数据不丢失；
f) 安全服务：为保障政务云全生命周期安全，应建立统一的安全管理、安全运维体系，保护云平台业务安全、数据安全和基础设施安全等；
g) 运管平台与接口要求。为政务云提供标准的接口，具备纳管相关物理设备及系统的能力。

6 技术要求

6.1 整体要求

政务云服务商提供的云平台应满足如下要求：
a) 整体可用性[1]不低于 99.99%，数据可靠性[2]不低于 99.9999%；
b) 政务云全部设备，包括服务器、网络设备、存储设备、安全设备等都应具备高可靠性及冗余性，即单个设备或单个节点出现故障时，其他设备/节点可立刻接管任务，保证云平台整体的业务连续性[3]不低于 99.99%。

6.2 机房环境要求

6.2.1 总体要求

总体要求如下：
a) 应满足国家 A 级机房标准 GB 50174-2008（2018 年 1 月 1 日以前设计）或 GB 50174-2017（2018 年 1 月 1 日以后设计）的要求；
b) 地址应位于本市行政范围内；
c) 应配备建筑与结构系统、供电系统、制冷系统、安防系统、智能监控系统、网络与布线系统及消防系统；
d) 应具备为特殊用户需求划分独立物理区域的能力；
e) 机房有较好的容灾备份方案及措施，若某一地区发生不可抗力灾害，容灾机房能快速、有效承接原服务。

6.2.2 基本要求

基本要求如下：
a) 新投产机房实际运行 PUE 不高于 1.3；
b) 机房采用市电双回路电源供电，提高供电保障和保护能力；
c) 可用性应达到 99.9%；
d) 应设安防监控系统、场地环境与设备监控系统、火灾报警系统、自动控制系统并能够实时监控场地运行数据，视频监控数据保存不小于 3 个月；其他数据保存不小于 12 个月；

注 1：整体可用性关注的是系统/服务能不能正常提供功能，以及正常运行的时间占比，针对的是系统的运行状态。
注 2：数据可靠性关注的是数据本身的准确性、完整性、一致性，以及数据被正确读取/写入/存储的能力，针对的是数据的质量和可信度。
[3]注 3：指云平台能够持续提供核心业务服务，或在服务中断后快速恢复核心服务，且不对用户业务造成实质性影响的能力。

e) 机房不得在居住场所或对外经营性场所楼内，且与最近的居住场所或大型经营性场所距离不小于 50 米；
f) 容灾机房与主机房之间距离须保证不低于 20 公里，容灾机房与主机房之间须采用两路冗余光纤或专线进行互联，且容灾机房与生产机房不能处于同一供电站供电范围；
g) 机房具有 UPS 系统保障能力，UPS 电池满负荷放电时间不少于 30 分钟；
h) 每机柜提供双路不间断供电，电力总功率每机柜不低于 3KW。

6.3 基础设施要求

6.3.1 计算要求

6.3.1.1 计算资源要求

计算资源提供的数据处理能力，一般要求如下：

a) 云主机应实现物理机的全部功能，如具有 CPU、存储、内存、网卡等资源，可以指定单独的 IP 地址、MAC 地址等；
b) 应支持存储裸设备映射（RDM），可以将存储设备上的 LUN 直接映射给虚拟机使用，并且支持 SCSI 指令使用透传模式或者非透传模式；
c) 应满足云主机之间、CPU 之间隔离保护要求；
d) 应支持资源的动态调整，根据业务的负载情况实现业务系统虚拟机的动态扩展和回收，支持手动和自动方式，自动方式可基于主机的 CPU、内存、磁盘 IO 等性能参数阈值进行动态调度；
e) 应支持在线进行虚拟化软件版本升级，不同版本之间可以相互兼容；
f) 应支持异构虚拟化能力，如 KVM、PowerVM 等多种虚拟化技术；
g) 云主机出现故障时，应支持自动重启或者迁移，保障业务连续性；
h) 应支持虚拟机热迁移，可在不同代 CPU 资源池中进行虚拟机热迁移；
i) 物理服务器 CPU 主频应不低于 2.0GHz；
j) 可用性不低于 99.99%。

6.3.1.2 虚拟机服务要求

计算资源应按照X86架构和ARM架构提供不同规格的虚拟机，包括小型虚拟机、中型虚拟机、大型虚拟机等。

a) 小型虚拟机（X86 架构）要求：vCPU≥2 个，内存≥8GB，硬盘≥50GB，CPU 主频≥2.2GHz，硬盘读写速度≥600 IOPS，并配置千兆网卡。
b) 小型虚拟机（ARM 架构）要求：vCPU≥2 个，内存≥4GB，硬盘≥100GB，CPU 主频≥2.0GHz，硬盘读写速度≥600 IOPS，并配置千兆网卡。
c) 中型虚拟机（X86 架构）要求：vCPU≥4 个，内存≥16GB，硬盘≥100GB，CPU 主频≥2.2GHz，硬盘读写速度≥600 IOPS，并配置千兆网卡。
d) 中型虚拟机（ARM 架构）要求：vCPU≥4 个，内存≥8GB，硬盘≥100GB，CPU 主频≥2.0GHz，硬盘读写速度≥600 IOPS，并配置千兆网卡。
e) 大型虚拟机（X86 架构）要求：vCPU≥8 个，内存≥32GB，硬盘≥100GB，CPU 主频≥2.2GHz，硬盘读写速度≥600 IOPS，并配置千兆网卡。
f) 大型虚拟机（ARM 架构）要求：vCPU≥8 个，内存≥16GB，硬盘≥100GB，CPU 主频≥2.0GHz，硬盘读写速度≥600 IOPS，并配置千兆网卡。
g) 虚拟机应支持提供单位 vCPU（1 核）和单位内存（1GB）的定制化服务，以应对特殊业务场景资源需求。

6.3.1.3 裸金属服务要求

裸金属服务要求如下：

a) 计算资源应按照 X86 架构和非 X86 架构提供不同规格的裸金属服务；
b) 非 X86 架构应该包含 ARM、x86、LoongArch、SW64 等不同的指令集架构；
c) 应为裸金属服务提供可选配件，包括内存、磁盘、网卡、GPU 等，以应对特殊业务场景资源需求。

6.3.2 存储要求

6.3.2.1 存储资源要求

存储资源提供数据存储的能力，一般要求如下：

a) 应支持结构化数据、半结构化数据和非结构化数据等多种数据类型存储；
b) 应支持块存储、对象存储、文件存储等多种存储方法，满足数据备份、视频存储等不同应用场景使用要求；
c) 应支持存储资源扩展能力，例如：PB 级扩展；
d) 应支持磁盘容错技术，如磁盘故障后节点的自动平衡和重构、硬盘故障检测和处理、集群节点出现单盘故障时不影响业务运行等；
e) 应支持加密存储，使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；
f) 存储系统的读写带宽应不低于 10Gbps；
g) 存储采用 SAN 或分布式存储架构，进行全路径冗余设计，存储服务全年可用率高于 99.99%；
h) 应支持对存储空间的数据彻底销毁，对底层存储介质实现完全初始化，防止数据删除后被非法还原。

6.3.2.2 存储服务要求

存储资源应能提供多种存储服务，包括文件存储服务、FC-SAN 存储服务、IP-SAN 存储服务、对象存储服务、SSD 高性能存储服务等。

a) 文件存储服务要求：总体 IOPS≥10000，总体吞吐量≥3000Mbps；每客户端的 IOPS≥100，每客户端吞吐量≥30MB/s；
b) FC-SAN 存储服务要求：总体 IOPS 性能≥50000，总体吞吐量≥3000Mbps；每客户端的 IOPS≥800，每客户端吞吐量≥180MB/s；
c) IP-SAN 存储服务要求：总体 IOPS 性能≥20000，总体吞吐量≥3000Mbps；每客户端的 IOPS≥600，每客户端吞吐量≥140MB/s；
d) 对象存储服务要求：总体 IOPS≥15000，总体吞吐量≥3000Mbps；每客户端的 IOPS≥600，每客户端吞吐量≥100MB/s；
e) SSD 高性能存储服务要求：总体 IOPS 性能≥100000，总体吞吐量≥3000Mbps；每客户端的 IOPS≥20000，每客户端吞吐量≥350MB/s。

6.3.3 网络要求

6.3.3.1 网络系统要求

网络系统提供数据传输能力，一般要求如下：

a) 应具备多运营商网络接入服务的能力；
b) 数据中心组网架构设计可采用大二层网络架构，应支持云主机无障碍动态迁移；
c) 应采用集群部署网络控制，以保障升级时业务不中断；
d) 应实现自动化动态网络资源调配和隔离，应支持与互联网、电子政务外网及行业部门专网的连接；
e) 应支持 IPv6 地址分配，满足业务系统 IPv6 要求；
f) 应具备边界防火墙和 VPC 防火墙隔离能力，分别针对不同的流量进行安全策略防护与配置；
g) 应具备高可用虚拟 IP 能力，在集群或主备场景下，云主机可绑定高可用虚拟 IP，达到高可用访问效果；
h) 应采用双活网络架构，降低单点故障带来的稳定风险；
i) 应为入云系统划分安全区域，合理制定访问规则；
j) 云内骨干线路带宽不低于 10Gbps；
k) 服务器业务带宽不低于 10Gbps；
l) 平均可用性不低于 99.99%。

6.3.3.2 网络服务要求

网络系统应能提供不同类型的网络服务，如硬件负载均衡、软件负载均衡等。

a) 硬件负载均衡要求：10/100/1000 电口≥16 个，千兆光口≥4 个，万兆光口≥2 个；并发连接数≥1600 万；4 层每秒新建连接数(CPS)≥50 万，7 层每秒新建连接数（CPS)≥40 万，SSL 每秒新建连接数（CPS）≥3 万。
b) 软件级负载均衡要求：支持包含 TCP 协议和 UDP 协议的四层负载均衡，以及包含 HTTP 协议和 HTTPS 协议的七层负载均衡；支持对应用程序的健康状态检查。

6.3.4 托管服务要求

托管服务主要用于政务云使用单位将自行购置的服务器、网络设备、安全设备等专业设备托管放置在政务云服务商的机房内，由政务云使用单位自行维护的场景。

政务云服务商提供上架、供电、供冷、政务外网链路、巡检（设备外观、指示灯、声音、振动等）等托管维护服务，具体要求如下：

a) 网络服务的可用时间≥99.9%，电力供应的可用时间≥99.99%；
b) 应提供共享 1000Mb 电子政务外网网络，IP 地址由云管理平台分配；
c) 上架开通时间≤5 小时；
d) 应提供云平台内部管理网络的 KVM 远程管理功能；
e) 应提供 7X24 在线技术支持。

6.4 支撑软件要求

6.4.1 数据库

6.4.1.1 一般要求

数据库为政务业务应用等提供数据存储能力，一般要求如下：

a) 应支持关系型数据库及非关系型数据库；
b) 关系型数据库应支持集中式数据库与分布式数据库两种架构；
c) 应支持主流的商业、开源操作系统，包括主流国产数据库；
d) 应支持数据库服务化管理，提供数据库全生命周期的管理能力；
e) 应支持对数据库监控、告警等。

6.4.1.2 关系型数据库

关系型数据库是指采用了关系模型来组织数据的数据库，其以行和列的形式存储数据。

a) 集中式的关系型数据库要求如下：
   1) 应具备基于集群及负载均衡等技术的能力；
   2) 应支持多种资源部署模式，如裸金属、云主机、容器等；
   3) 应具备数据库的备份能力与集群的容灾能力。
b) 分布式的关系型数据库要求如下：
   1) 事务型数据库应能抵御网络问题导致分布式数据库服务脑裂风险；应支持跨库死锁检测；应支持数据分片在线拆分；
   2) 分析型数据库应支持对时序数据进行存储和分析，应支持标准云原生存算分离架构。
c) 关系型数据库提供 RDS 单机版、HA 版、RAC 版三种类型。
   1) HA 版本使用一主一备的高可用架构，当主服务器故障时，实例会自动切换到备服务器运行；
   2) HA 主备版要求 RTO≤3 分钟，RPO 小于等于 1GB；
   3) RAC 版本使用多节点的高可用并行架构，多个节点并行运行，任何单节点故障时，业务不受影响；
   4) RAC 版要求 RTO≈0，RPO=0。

6.4.1.3 非关系型数据库

非关系型数据库是基于高可用架构，满足高读写性能及快速数据访问需求的数据库，要求如下：

a) 应支持内存和硬盘的持久化存储方式；

b） 应支持多种资源模式部署，如：云主机、裸金属、容器等；
c） 应支持虚拟网络，指定虚拟网络创建内存数据库实例；
d） 应支持在线平滑升降级，计算能力、内存容量和总 I/O 带宽同步线性扩容；
e） 应支持缓存服务的容灾。

6.4.2 中间件

6.4.2.1 概述

中间件为业务提供应用支撑能力，包括应用服务器中间件、消息中间件等。

6.4.2.2 应用服务器中间件

应用服务器中间件要求如下：
a） 应支持多服务器群集部署、负载均衡，支持对多种对象的集群功能；
b） 应支持热部署、远程部署等多种部署方式；
c） 应支持异构集群技术，当硬件平台或操作系统不是同一产品时，应用服务器能建立异构集群；
d） 在业务系统不宕机的情况下，应支持动态增加服务器，扩充系统性能；
e） 应提供访问控制功能；
f） 应提供审计功能，实现对用户在系统的事件进行记录和存储，能够进行查询，能够对审计进行响应。

6.4.2.3 消息中间件

消息中间件要求如下：
a） 应提供消息优先级控制功能、提供消息生命周期控制功能；
b） 应支持发送队列、本地队列、远程队列、虚拟队列等；
c） 应支持用户根据实际情况灵活组织节点，组建需要的网络结构；
d） 应支持常连接和按需连接两种模式，以更好地适应不同的网络通讯环境，节省系统资源和提高传输效率；
e） 应支持断点续传，消息保留在消息队列中，等待系统恢复后，消息将从传输失败点继续发送；
f） 应支持多种分发模式的集群，若干个节点组成一个群组，统一对外提供消息接收和处理功能，且集群内的各个节点对于应用是透明的；
g） 应具有完整的日志功能，通过日志可以查看系统传输情况，消息的传输情况，并可以排除系统中出现错误信息。

6.4.3 操作系统

操作系统是支撑政务业务应用的服务之一，应为云主机、裸金属等云服务提供操作系统镜像服务，一般要求如下：
a） 应提供各类主流的商用、开源操作系统，包括主流国产操作系统，并确保操作系统使用的合法性、安全性；
b） 应提供基于不同 CPU 架构的操作系统，以适应不同业务应用需要；
c） 应具备适配新型操作系统的能力。

6.4.4 容器

6.4.4.1 资源管理

提供以容器为核心的容器管理服务，为容器化的应用提供高效部署、资源调度、服务发现等一系列完整功能，具体要求如下：
a） 应具备资源管理能力；
b） 应具备多集群管理能力；
c） 应具备多租户管理能力；
d） 支持将容器镜像共享给其他用户；
e） 应具备运维系统、监控系统等基本功能。

6.4.4.2 弹性伸缩

容器云服务提供以容器为核心的动态伸缩功能，具体要求如下：

a) 应提供资源分配与调度功能，包括统计资源利用率，并能够按照策略动态分配资源；
b) 应提供容器动态迁移功能，包括伸缩迁移、故障迁移等功能；
c) 应支持容器通过手工和自动方式的弹性伸缩。

6.4.5 运行监测

6.4.5.1 概述

运行监测服务解决用户业务系统间集成复杂、故障定位难、被动获取数据缺乏真实性等问题，实现辅助预警、态势感知、多系统间业务端到端调用过程回溯、划清责任边界的全面监控目标。

6.4.5.2 监控要求

监控要求如下：

a) 支持探针自动发现、自动监控主机、进程、服务；
b) 支持基于协议发现，自动梳理访问关系，形成应用、服务、业务拓扑，实现应用间复杂关系的可视化；
c) 提供直观、易用的可视化界面，包括实时监控数据、历史数据分析、趋势分析等；
d) 支持多维度、多视角的数据展示和分析，以全面了解业务系统的性能表现；
e) 支持通过可视化及各类监控数据，对性能瓶颈进行分析排查，找出性能瓶颈或故障原因；
f) 能够根据预设的警报阈值发送通知或警报。

6.5 业务应用要求

6.5.1 网盘服务要求

网盘服务要求如下：

a) 网盘服务应包含多维度存储空间、多终端支持、同步盘功能、文件协作共享、文件快速迁移、数据摆渡、敏感内容检测、空间容量预警、文件历史版本管理、文档安全备份、多级权限管控、文件水印；
b) 应具备海量数据检索能力，能够提供多维度的检索，可以最大程度的处理数据的分析与检索；
c) 应支持一主一备备份机制，保证各个区域保留多个副本保证数据一致与数据安全，当主库故障时，自动完成主从切换，确保业务服务不中断，避免单点故障；
d) 应提供不少于 2 副本方式保障数据安全，保证存储数据的完整性、安全性；
e) 应提供离线备份能力，根据策略定期对系统数据和海量文件进行异地备份，备份过程不影响业务正常运行。

6.5.2 BI 数据服务要求

BI数据服务要求如下：

a) BI 数据服务应提供多维分析和报表展现，快速获得分析结果；
b) 应支持多种数据源的集成，能够将不同数据源的数据汇总到一个仪表板中进行统一的分析；
c) 应支持多种数据可视化选项，如图表、图形和地图等，能够将数据以直观和易于理解的方式呈现给用户；
d) 应支持多用户的界面，使用户能够通过简单的拖放和筛选等方式轻松创建自定义报表和分析；
e) 应支持实时数据更新和分析；
f) 应支持权限控制功能，确保只有授权用户才能访问敏感数据。

6.6 容灾备份要求

6.6.1 容灾服务要求

容灾服务要求如下：

a) 应提供同机房跨存储设备的数据容灾服务；

b） 应提供实时同步、实时异步、分钟级定时保护策略；
c） 当业务系统因故障停止服务时，应急接管并恢复业务＜10 分钟，保障业务数据不丢失；
d） 应急接管服务存储空间应与生产区业务系统所使用的存储资源池物理隔离；
e） 应支持分布式数据库集群或业务集群的整体一致性恢复接管。

6.6.2 备份服务要求

备份服务要求如下：
a） 备份介质本身具备高可用性和冗余性；
b） 备份方式应包括完整备份、差异备份和增量备份；
c） 备份服务全年可用率≥99.9%；
d） 备份时不对数据库和文件的存取和写入造成很大性能影响，不能导致虚拟机、物理机低于最低指标；
e） 备份恢复应以用户为单位做隔离，每个用户只能访问自己备份数据；
f） 虚拟机镜像服务采用虚拟化层备份技术，无需在虚拟机中安装备份客户端，提供增量、差异、全量备份功能；
g） 针对主流虚拟化平台，支持直接挂载备份集即可实现虚拟机的快速恢复。

6.7 安全要求

6.7.1 总体技术要求

政务云平台总体要求如下：
a） 应保证安全技术服务能力不低于所承载的信息系统的最高级别，并通过 GB/T 22239 相应等级的测评；
b） 应符合 GB/T 34080.1，GB/T 34080.2，GB/T 34080.3，GB/T 34080.4 中的规定；
c） 应通过商用密码应用安全性评估，商用密码应用安全性评估参考 GB/T 39786-2021 中相应等级规定；
d） 应保障其上的租户安全、容器安全、云主机安全、业务安全和数据安全。

6.7.2 虚拟防火墙

虚拟防火墙具体要求如下：
a） 应支持虚拟机形式交付，支持 KVM 等主流虚拟化平台；
b） 应云平台安全管理接口、虚拟设备管理接口；
c） 防火墙最大吞吐量≥2Gbps；
d） IPsecVPN 数量≥50 个；
e） VPN 最大吞吐量≥200Mbps，SSL VPN 用户数≥250；
f） 最大并发会话数≥500K，每秒新建连接数≥20K；
g） 应支持 NAT，包括动态和静态地址转换；
h） 应支持各类主流路由协议，等价路由、策略路由；
i） 应支持基于状态、精准的高性能攻击检测和防御；
j） 应支持实时攻击源阻断、IP 屏蔽、攻击事件记录；
k） 应支持基于策略或者安全域的入侵防范，可针对不同的服务器对象定制不同的规则集合。

6.7.3 应用层防火墙（WAF）

应用层防火墙（WAF）具体要求如下：
a） 虚拟机形式交付，支持 KVM 等主流虚拟化平台；
b） 支持代理、路由牵引等模式；
c） 云平台安全管理接口、虚拟设备管理接口；
d） Web 攻击检测特征数≥3000 条；
e） 支持检测和防御 OWASP 定义 10 大 web 安全威胁（如 SQL 注入防护、XSS 攻击防护、CSRF 攻击防护）；

f) 支持对常见 Web 建站内容管理系统的防护，所支持的 CMS 类型数量≥20 种；
g) 支持基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力；
h) 支持访问速率和访问集中度检测算法。

6.7.4 web 防篡改服务

web防篡改服务具体要求如下：
a) 上传文件速度≤5ms（50K 文件）；
b) 篡改恢复时间≤6ms；
c) 篡改检测时间：访问时实时检测；
d) 支持外挂轮询、核心内嵌及文件驱动过滤三种篡改检测技术；
e) 支持通过在网页被访问时进行完整性检查杜绝网站向外发送被篡改的页面内容；
f) 支持预先禁止非法程序对备份/保护目录的添加/删除/修改/更名/属性变更等操作；
g) 能够防护 SQL 数据库注入式攻击；
h) 能够防护跨站脚本漏洞；
i) 规则库采用正则表达式描述，规则扩展性高。

6.7.5 主机漏洞检测服务

主机漏洞检测服务具体要求如下：
a) 检测漏洞数≥15000；
b) 检测配置检查项数≥2000；
c) 能够全面发现信息系统存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告；
d) 能够快速定位风险类型、区域、严重程度，直观展示安全风险；
e) 能够结合安全管理制度，支持安全风险预警、检查、分级管理、修复、审计流程，并监督流程的执行；
f) 能够提供多种灵活部署方式，适应复杂的网络环境下的部署，并尽量控制降低安全建设成本。

6.7.6 主机防病毒服务

具体要求如下：
a) 支持智能识别蠕虫或者木马软件，无需提示用户操作判断；
b) 支持对安全风险检测有详细的分类，同时有灵活的处理方式，包括清除、隔离；
c) 支持提供病毒隔离系统，将染毒文件安全隔离；
d) 防（杀）病毒软件能够自动隔离感染而暂时无法修复的文件。

6.7.7 数据库审计

具体要求如下：
a) 应支持同时审计多个数据库，实时监测解析数据库的登录、退出、插入、删除、执行存储过程等操作，能够准确完整还原 SQL 操作语句；
b) 应支持数据库操作类、表、表空间、函数、程序包、事物、cluster、别名、视图、索引、触发器、域、存储过程等各种对象的变更、创建、授权、删除操作的 SQL 操作审计；
c) 应支持对超长 SQL 操作语句审计；
d) 应支持对数据请求的报文进行审计，同时支持返回结果审计，特别是数据库返回的内容；
e) 可基于会话、风险、语句分布等多维度，进行趋势分析与统计，并以图表结合的方式进行展现；
f) 应支持对磁盘进行预警阀值和保护阀值的设定，当磁盘容量超过保护阀值条件时系统提供覆盖和停止操作对磁盘进行保护。

6.7.8 日志审计

具体要求如下：

a) 应支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、SFTP 协议日志收集；
b) 应支持使用代理(Agent)方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导；
c) 应支持通过基于日志内容深度分析的日志专家规则库，对采集到的日志数据进行实时动态分析，将网络非法访问、数据违规操作、系统进程异常、设备故障等高危安全事件，从海量日志数据中提取出来；
d) 应支持日志数据异地备份和自动归档功能，并且归档文件通过加密方式存储，以保证日志数据的完整性、安全性和可用性；
e) 应提供丰富的合规性报表模块（如 SOX 法案、等级保护），满足用户的日常审计需求；
f) 应支持手动/自动报表功能，支持用户多条件组合生成报表；
g) 应支持对 Agent 进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。

6.8 运管平台与接口要求

6.8.1 云管平台要求

政务云服务商应整合多个异构资源池，在资源池层面提供计算虚拟化、存储虚拟化、网络虚拟化等能力，在运营层面提供资源调度、资源监控、资源告警、高可用等能力，并开放API接口，满足以下基本技术要求：

a) 支持虚拟机的生命周期管理，包括创建、删除、修改配置、查找搜索、快照、克隆等；
b) 支持监控所接入的存储池的利用率监控，支持利用率阈值告警；
c) 支持监控虚拟机、计算节点的 CPU、内存、存储使用率等指标，支持按照支持天/周/月/年维度展示；
d) 支持监控数据保留≥1 年；
e) 支持跨计算节点热迁移，支持跨存储迁移；
f) 支持集群高可用，当某计算节点发生故障时，所承载的虚拟机能在其他计算节点重新启动，全程无需干预，要求 RTO 指标小于 10 分钟。

6.8.2 平台接口要求

6.8.2.1 概述

政务云平台应提供标准的接口，包含但不限于管理平台、虚拟化平台、网络、安全、存储系统等接口，具备纳管相关物理设备及系统的能力，提供标准的南向接口和北向接口功能及标准文档规范。

6.8.2.2 南向接口

南向接口主要是基础设施层的接入，对云资源和服务进行统一纳管，包含但不限于：

a) 硬件接入要求：应提供物理设备的接口，包括服务器设备、网络设备、存储设备等；
b) 软件接入要求：
    1) 应遵循 Restful 风格，可以查询政务云平台服务状态信息、云平台物理资源使用情况等；
    2) 应提供政务云使用单位相关的增、删、改、查等接口；
    3) 应提供云主机的相关接口，包括虚拟机云主机详细信息、列表、快照、硬盘规格、镜像等；
    4) 应提供存储资源相关的接口，包括云硬盘、硬盘快照、访问鉴权等；
    5) 应提供虚拟网络资源相关的接口，包括网络、子网、网卡、虚拟路由、安全组、公网 IP、VFW、VPN、VLB 等。

6.8.2.3 北向接口

北向接口主要是云管理平台的开放接口，以实现云管平台能够被第三方应用开发、部署和安全监管，包含但不限于：

a) 应提供丰富的 REST API 接口供第三方在云操作系统上进行业务应用开发部署，提供的接口涵盖基础设施、支撑软件和业务应用各个层面，实现一个开放的云服务平台；

b) 应提供多种安全监管接口，以提供相关安全监管数据。安全监管接口类型包括网络流量接口、网络协议接口、云主机接口和 API 等。

6.9 其他要求

6.9.1 扩展能力要求

扩展能力是指满足当前建设要求的前提下，具备按照政务云管理单位要求、政务云使用单位要求进行扩展开发的能力，一般包括：云平台扩展、系统对接扩展等。

6.9.1.1 云平台扩展要求

云平台扩展能力是指，根据政务云管理单位、政务云使用单位的要求，对云管理平台进行相应扩展开发的能力，一般要求如下：

a) 应支持云服务统一门户，支持统一的接入入口与现有的业务系统进行集成；
b) 应支持大屏展示模块，包括政务云运行状态、资源情况、运维事件等展示功能；
c) 应支持大屏扩展模块，包括多维度指标的按需展示和用户自定义编排；
d) 应支持运维管理模块，包括租户和管理员门户、监控、报表等的按需开发，并支持自定义展示；
e) 应支持运营模块，包括申请审批流程、组织管理、多级审批等按需开发。

6.9.1.2 系统对接扩展要求

系统对接扩展能力是指：根据云管理单位、使用单位的要求，对云管理平台与其他系统进行对接，不断拓展政务服务能力，一般要求如下：

a) 应支持标准的 REST 风格 API 接口，通过接口将各服务商提供的各项功能与其他平台进行互联互通；
b) 应具备第三方设备的异构兼容开发能力，包括硬件、安全设备等；
c) 应具备第三方产品的快速部署对接能力，包括 SaaS 类应用的镜像上传、安装部署和运维监控等能力；
d) 应具备第三方管理平台的对接能力，包括安全管理、运维管理、监管平台等；
e) 应具备生态场景的对接能力，包括平台设施、中间件、数据库、业务逻辑、UI 等；
f) 应提供对接操作的规范性流程，包括：
    1) 明确业务过程，明确政务云服务与第三方服务之间业务关系；
    2) 明确接入方式，如协议方式、SDK 方式等；
    3) 明确接口信息，应根据业务场景，明确需要接口调用的具体数据信息；
    4) 制定规范性文档，根据以上三条 1)-3)，与第三方平台沟通确认后，制定接入规范性文档，政务云服务根据接入规范进行对接；
    5) 接入联调，按规范性文档，接入第三服务，并对接入的服务进行双方联调；
    6) 接入完成，根据请求信息完成配置后，完成接入。

6.9.2 运营服务要求

政务云平台运营的人员管理、服务目录管理、服务级别管理、服务请求管理、服务报告管理、自服务管理、用户管理、计费管理等应遵循GB/T 36326的相关规定。

政务云服务商应做好上架云服务的计量、计费、资源统计、分析与优化等服务全生命周期的运营工作，包括：

a) 应支持对计算资源、网络资源、存储资源、安全资源自动化调度及管理；
b) 应对云资源使用情况进行计量管理；
c) 应支持云资源账单记录、费用预估和分析等管理；
d) 应支持资源总览、使用分析、整体优化等活动；
e) 应提供服务目录、工单管理、报表管理、权限管理、运行数据管理和汇集等功能。

云服务商宜结合使用单位的实际需要和采购需求，以扩展服务等形式提供运营支持，包括：

a) 应用系统上云：提供应用兼容性评估、上云基础架构设计、上云实施技术支持、迁移风险策略控制等服务；
b) 云上应用调优：提供应用架构诊断、分库分表设计、微服务治理、云原生改造等服务；
c) 全链路压测：提供压测方案设计、实施支持、优化服务等服务；
d) 重大活动护航：提供深度健康检查、预防式维护、应急保障计划、高级别现场维护与故障处理等服务。

6.9.3 数据汇集要求

6.9.3.1 概述

政务云服务商应在政务云管理部门的授权下，向政务云综合监管服务商提供汇集数据，用于开展监管工作。汇集数据应结合云管理单位的管理目标和内容进行详细定义，可通过政务云平台监管数据汇集接口进行数据汇集。数据汇集规范相关示例详见附录A。

6.9.3.2 政务云平台监管数据汇集接口

政务云平台监管数据汇集接口按形式可分为网络流量接口（NFLOWI）、网络协议接口（NPROTI）、云主机接口（VMI）和应用程序编程接口（API）4种类型。获取运行监管信息和交付件的方式包括：手工机制和自动机制。政务云综合监管服务商通过监管接口获取数据信息对政务云服务商进行持续监管，也可通过手工机制来实现。自动化机制的监管接口框架如图6所示。

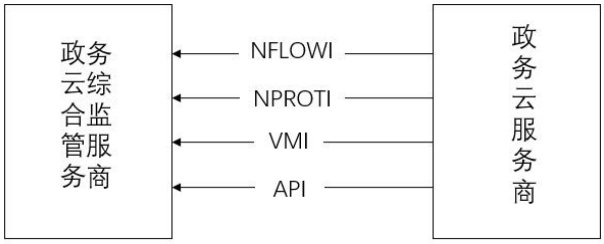

图 2 政务云平台监管数据汇集接口框架图

6.9.3.3 资产数据

包括但不限于物理环境资产、物理设备资产、云主机资产、IP资产、用户资产（入云系统）等，实现对各类资产状态和数量的实时监控。

6.9.3.4 机房环控数据

包括但不限于温湿度传感器、门禁、发电机、电池监控模块、UPS等。

6.9.3.5 云平台数据

包括但不限于云平台规格数据、云平台网络接入IP数据等。

6.9.3.6 应用数据

包括但不限于业务系统数据、云主机规格数据、互联网链路带宽服务数据等。

6.9.3.7 监控数据

包括但不限于运行监控数据、应用系统网络出口使用数据、VPN/远程接入登录数据等.

6.9.3.8 日志数据

包括但不限于安全设备日志和主机日志等。

附 录 A
（资料性）
云平台数据汇聚规范（示例）

A.1 政务云平台监管数据汇集接口

政务云平台监管数据汇集接口如表A.1所示。

表 A.1 政务云平台监管数据汇集接口

云平台接口	接口分类	要求描述	数据汇集结果
网络流量接口 NFLOWI	物理网络接口	政务云服务商应提供云计算平台物理网络中核心交换机和接入交换机的物理网络接口流量，用于监测、审计云计算平台安全事件等综合监管工作	网络协议数据
	虚拟网络接口	政务云服务商应提供云计算平台的虚拟交换和路由设备接口，以获取设备中使用的协议列表、源 IP 地址列表、目标 IP 地址列表、服务端口、数据流向等信息。所提供的虚拟交换和路由设备接口应支持将指定流量根据指定策略牵引到政务云综合监管服务商的设备，用于监测、审计等工作	网络协议数据
网络协议接口 NPROTI	Syslog接口	政务云服务商应开启云计算平台物理网络中服务器、网络设备、安全设备等的 Syslog 接口，通过网络将syslog消息发送到云监管服务商的设备	日志数据
	SNMP接口	政务云服务商应开启云计算平台网络、安全设备的SNMP协议管理接口，使得政务云综合监管服务商获取所有网络安全设备的运行信息	日志数据
	以太网接口	政务云服务商应为政务云综合监管服务商分配合适的以太网接口，保证云监管能监测到监管对象，政务云综合监管服务商可通过以太网口接入云计算平台网络，开展云平台安全监管工作	/
云主机接口VMI	云主机接口	政务云服务商应提供虚拟云主机接口用于对虚拟资源性能状况进行抽样监测	/
应用程序编程接口 API	应用程序编程接口	政务云服务商应根据综合监管工作的需要，按需提供 API 接口，以便获取支撑综合监管工作开展的基础数据。（API接口依据云管理单位的实际要求，选择自动机制或者手工机制）	资产数据 机房环控数据 云平台数据 应用数据 监控数据

A.2 资产数据

汇总云服务商云平台物理资产数据如表A.2所示。

表 A.2 资产数据

数据分类	数据内容描述	范围
物理环境/设备资产	云平台物理设备名称、设备 S/N（序列）号、品牌名称、设备型号、硬件规格、IP 地址、设备所在机房、所在机柜、设备功率、电源类型、设备所有单位、设备管理单位、运行状态、启	物理环境资产：包括机房、机柜等。 物理设备资产：包括服务器、存储、网络交换、安全设备等

	用日期、撤出日期等	
云主机资产/用户资产	入云系统名称、虚机资产、IP 地址、使用单位系统管理人员、管理员联系方式、系统入云时间、服务启用/撤离时间	云平台的入云系统和云主机资源使用情况

A.3 机房环控数据

机房环控数据如表A.3所示。

表 A.3 机房环控数据

数据分类	数据内容描述
温湿度传感器	设备所在机房、所在位置、温度数据、湿度数据
发电机	设备编号、所在位置、故障状态、油位容量、运行状态
电池监控模块	设备编号、所在机房、所在位置、电流数据、总电压数据、后备时间
UPS	设备所在机房、所在位置、输入频率、环境温度数据、环境湿度数据、输出频率、电池总电压、电池总电流、电池温度、电池后备时间、电池剩余容量、电池总电流、UPS 供电状态、UPS 运行状态、电池运行状态、市电输入告警状态、电池告警状态
采集器	设备所在机房、所在位置、漏水状态、红外状态、继电器输出数据
列头柜	设备所在机房、所在机柜编号、A/B/C 相电压、A/B/C 相电流、A/B/C 相负载率
电量仪	设备所在机房、所在位置、总有功电度量、总无功电度量

A.4 日志数据

采集云平台物理网络中的安全设备日志、云主机日志数据，如表A.5所示。

表 A.4 网络协议数据

数据分类	数据内容描述
安全设备日志	日志产生日期、日志报警名称、安全设备发生源 IP、安全设备代理 IP、安全设备名称、设备 S/N 号、设备类型、源 IP 及端口、目的 IP 及端口、日志等级、报警类型、日志内容
主机日志	云主机日志（例如创建）产生日期、云主机 ID、主机名称、主机 IP、操作系统类型、日志名称、日志类型、日志正文内容

A.5 云平台数据

政务云服务商提供云平台的整体管理数据，如表A.6所示。

表 A.5 云平台数据

数据分类	数据内容描述
云平台规格数据	云服务商名称、设备所在机房、云平台产品供应商、云平台网络类型（政务外网/互联网）、CPU 总量、CPU 分配量、内存总量/分配量、普通存储总量/分配量、高性能存储总量/分配量、静态存储总量/分配量、互联网带宽总量/分配量

云平台网络接入 IP 数据	网络类型（政务外网/互联网）、云服务商名称、设备所在机房、网络运营商、IP 地址/IP 地址段、主链路带宽数、备份链路带宽数

A.6 应用数据

政务云服务商统计云平台入云信息系统的基本情况，如表A.7所示。

表 A.6 应用数据

数据分类	数据内容描述
业务系统数据	政务云使用单位编号、单位地址及邮编、云服务商名称、所属节点、设备所在机房、信息系统编号、入云测试日期、系统联系人姓名、系统联系人手机号、系统联系人邮件地址、系统联系人座机、技术联系人姓名、技术联系人手机号、前置审批情况、系统功能描述、系统等保级别、运行时间要求、系统服务对象、系统服务范围、所属网络类型（政务外网/互联网）、系统互联网情况及涉及单位、上线日期、退出日期、退出原因、系统 IP 地址、系统开发商名称
云主机规格数据	信息系统编号、云主机名称、云主机 ID、内部 IP、云主机类型、云主机运行状态、云平台所属服务商、云主机设备所在机房、云主机所属网络类型（政务外网/互联网）、云主机创建/删除日期、CPU 核数、内存分配量、平台存储分配量、高性能存储分配量、本地视频存储分配量、异地存储分配量、云主机深度监控服务情况
互联网链路带宽服务数据	信息系统编号、互联网 IP、系统域名、互联网带宽数、互联网带宽接入起始时间、互联网带宽接入截止时间
主机负载均衡服务数据	信息系统编号、内网 IP、外网 IP、负载 IP、开放端口、负载开通日期、负载关闭日期
VPN 服务数据	信息系统编号、VPN 类型、账号名称、可访问范围（IP 或 IP 地址段）、VPN 开通日期、VPN 关闭日期
WAF 防护服务数据	信息系统编号、WAF 所防护 IP 地址及端口号、WEB 防护类型（默认或自定义）、WAF 防护开通时间、WAF 防护关闭时间
远程接入服务数据	信息系统编号、远程接入账号名称、可访问范围（IP 或 IP 地址段）、远程接入开通日期、远程接入关闭日期
云机房专线接入服务数据	信息系统编号、网络运营商、专线用途、专线接入起始时间、专线取消结束时间、线路本端（云平台端）地址、线路对端地址、配线柜编号、云机柜编号、接入设备名称及端口号

A.7 监控数据

向政务云监管单位提交云平台的管理数据如表A.8所示。

表 A.7 监控数据

数据分类	数据内容描述
云主机监控数据	云主机ID、监控数据时间、云主机内部IP地址、CPU使用率、内存使用率、普通存储使用率、高性能存储使用率、静态存储使用率、本地视频存储使用率、异地视频使用率、磁盘写峰值、磁盘读峰值、带宽上行峰值、带宽下行峰值

数据分类	数据内容描述
应用系统网络出口使用数据	信息系统编号、连接网络类型（政务外网/互联网）、监控数据时间、带宽上行峰值、带宽下行峰值
VPN/远程接入登录数据	信息系统编号、连接网络类型（政务外网/互联网）、监控数据时间、VPN远程接入类型（SL VPN/Ipsec VPN）、远程接入账号、会话ID、登入时间、退出时间
运维监测数据	运维监测类型（机房巡检、云平台运维、网络运维、安全运维）、监测内容、状态（是否正常）、监测时间、监测人
安全漏洞扫描数据	安全漏洞名称、漏洞类型（主机漏洞、数据库漏洞、WEB漏洞、中间件及其他组件漏洞等）、安全漏洞风险等级、漏洞存在的云主机ID、所属信息系统名称、扫描时间、漏洞通知情况（是否已联系系统责任人）、漏洞整改情况、漏洞整改时间
安全补丁安装数据	安全补丁名称、安装补丁的云主机ID、补丁类型（Windows补丁、Linux补丁、国产操作系统补丁、各类数据库补丁、中间件补丁）、安全补丁发布时间、安全补丁安装时间、监测人
安全预警监测数据	监测类型（漏洞发布/补丁发布）、监测内容、预警情况（是否已通知相关单位）、监测时间、监测人
安全攻击监测数据	安全攻击名称、攻击涉及云主机ID、攻击涉及信息系统编号、安全攻击通报情况（是否已通知相关单位）、监测时间、监测人

参 考 文 献

[1] GB/T 31168—2023 信息安全技术 云计算服务安全能力要求
[2] GB 50174 数据中心设计规范